This listing of the claims will replace all prior versions and listings of claims in the application:

LISTING OF THE CLAIMS

Claim 1 (currently amended). A method of recording and printing user data on a printed medium, comprising the steps of:

a. encoding the user data to form an encoded user data array **A**;

b. modulating the user data array **A** using a two-dimensional pseudo-random kernel $\mathbf{K}_m$, to form a modulated data array **E**;

c. formatting the data array **E** to produce a pixel-based two-dimensional barcode array **B**; and

d. printing the barcode array **B** onto a portion of the printed medium,

wherein the recorded and printed user data is distributed evenly across said portion of the printed medium such that each pixel of barcode array **B**, on average, contains an equal fraction of the user data.

Claim 2 (previously presented): The method of claim 1, wherein the user data is encoded so that the user data array **A** additionally comprises a fiducial signature.

Claim 3 (original): The method of claim 2, wherein the fiducial signature comprises a recognizable signature texture and a signature pattern.

Claim 4 (previously presented): The method of claim 1, further comprising step (e) superimposing onto the barcode array **B** a formatted version of a two-dimensional signature array **C**.

Claim 5 (previously presented): The method of claim 4, wherein in step (a), the user data is encoded so as to have a signature texture incorporated therein, and further wherein the signature array **C** contains a signature pattern bitmap modulated using a two-dimensional pseudo-random kernel $\mathbf{K}_c$.

Claim 6 (original): The method of claim 5, wherein the two-dimensional kernels $\mathbf{K}_m$ and $\mathbf{K}_c$ are the same.

Claim 7 (previously presented): The method of claim 4, wherein the signature array **C** comprises a signature texture array modulated using a two-dimensional pseudo-random kernel $\mathbf{K}_c$.

Claim 8 (previously presented): The method of claim 4, wherein in step (a) the user data is encoded so as to have a signature pattern incorporated therein, and further wherein, the signature array **C** contains a signature texture modulated using a two-dimensional pseudo-random kernel $\mathbf{K}_c$.

Claim 9 (previously presented). The method of claim ~~9~~8, wherein the two-dimensional pseudo-random kernels $\mathbf{K}_c$ and $\mathbf{K}_m$ are the same.

Claim 10 (previously presented): The method of claim 1, further comprising in combination with step (c) formatting and superimposing onto the formatted data array **E** a second two-dimensional modulated data array **E'**, wherein the data array **E'** is produced by modulating a second data set with a second two-dimensional pseudo-random kernel, $\mathbf{K'}_m$ and the barcode array **B** is produced by the superimposition of the formatted data array **E'** onto the formatted data array **E**.

Claim 11 (currently amended): A readable barcode made using ~~the~~a method ~~of claim 1~~ comprising the steps of:

a. encoding user data to form an encoded user data array **A**;

b. modulating the user data array **A** using a two-dimensional pseudo-random kernel $\mathbf{K}_m$, to form a modulated data array **E**;

c. formatting the data array **E** to produce a pixel-based two-dimensional barcode array **B**; and

d. printing the barcode array **B** onto a portion of a printed medium,

wherein the recorded and printed user data is distributed evenly across said portion of the printed medium such that each pixel of barcode array **B**, on average, contains an equal fraction of the user data.

Claim 12 (currently amended): ~~A~~The readable barcode ~~made using the method of claim 2~~of claim11, wherein the user data is encoded so that the user data array **A** additionally comprises a fiducial signature.

Claim13 (currently amended): ~~A~~The readable barcode ~~made using the method of claim 4~~of claim 11, wherein the method further comprises step (e) superimposing onto the barcode array **B** a formatted version of a two-dimensional signature array **C**.

Claim 14 (original): The readable barcode of claim 13, wherein up to approximately 80% of the barcode has been obfuscated.

Claim 15 (original): The readable barcode of claim 14, wherein the obfuscation is caused by overlaid text or graphics.

Claim 16 (original): The readable barcode of claim 14, wherein the obfuscation is caused by damage or partial destruction of the printed medium.

Claim 17 (previously presented): A method of reading user data stored on a printed medium according to the method of claim 1, comprising;

a. scanning the barcode array **B** to obtain the data array **E**;

b. demodulating the data array **E** with a two-dimensional pseudo-random kernel $\mathbf{K}_d$ that is related to the two-dimensional pseudo-random kernel $\mathbf{K}_m$, to obtain the user data array **A**; and

c. decoding the user data array **A** to obtain the encoded user data.

Claim 18 (previously presented): A method of reading user data stored on a printed medium according to the method of claim 2, comprising;

a. scanning the barcode array **B** to obtain an uncorrected version of data array **E**;

b. demodulating the data array **E** with a two-dimensional pseudo-random kernel $\mathbf{K}_d$ that is related to the two-dimensional pseudo-random kernel $\mathbf{K}_m$, to obtain an uncorrected version of the user data array **A**;

c. transforming the uncorrected version of the user data array **A** using the fiducial signature contained therein to produce a corrected version of the user data array **A**; and

d. decoding the corrected version of the user data array **A** to obtain the encoded user data.

Claim 19 (previously presented): A method of reading user data stored on a printed medium according to the method of claim 4, comprising;

a. scanning the barcode array **B** to obtain a raw scan;

b. demodulating the raw scan with a two-dimensional pseudo-random kernel $\mathbf{K}_c$ that is not related to the two-dimensional pseudo-random kernel $\mathbf{K}_m$, to obtain an uncorrected version of the signature array **C**;

c. transforming the raw scan using the uncorrected version of signature array **C** to obtain a corrected version of data array **E**;

d. demodulating the corrected version of data array **E** with a two-dimensional pseudo-random kernel $\mathbf{K}_d$ that is related to the two-dimensional pseudo-random kernel $\mathbf{K}_m$, to produce a corrected version of the user data array **A**; and

e. decoding the corrected version of user data array **A** to obtain the encoded user data.

Claim 20 (previously presented): The method of claim 19, wherein steps (a) through (c) are performed iteratively on subsections of the barcode array **B** and the signature array **C** contains a signature texture and a signature pattern.

Claim 21 (previously presented): A method of reading user data stored on the barcode of claim 14 comprising the steps of

a. scanning the barcode array **B** to obtain a raw scan;

b. thresholding the raw scan;

c. demodulating the thresheld raw scan with a two-dimensional pseudo-random kernel $\mathbf{K}_c$ that is not related to the two-dimensional pseudo-random kernel $\mathbf{K}_m$, to obtain an uncorrected version of the signature array **C**;

d. transforming the raw scan using the uncorrected version of the signature array **C** to obtain a corrected version of the data array **E**;

e. demodulating the corrected version of the data array **E** with a two-dimensional pseudo-random kernel $\mathbf{K}_d$ that is related to the two-dimensional pseudo-random kernel $\mathbf{K}_m$ but not related to the two-dimensional pseudo-random kernel $\mathbf{K}_c$, producing a corrected version of the user data array **A**; and

f: decoding the corrected version of the user data array **A** to obtain the encoded user data.

Claim 22 (previously presented): The method of claim 21, further comprising iteratively repeating step (c) on subsections of the barcode array **B** and the signature array **C** contains a signature texture and a signature pattern.